

# Kernels of modular inclusion maps

I.J. Siemons\*

*School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK*

Received 30 November 1994; revised 10 August 1995

---

## Abstract

Let  $R$  be a field and  $\Omega$  an  $n$ -element set. For  $k \leq n$  consider the  $R$ -vector space  $M_k$  with  $k$ -element subsets of  $\Omega$  as basis. The inclusion map  $\partial: M_k \rightarrow M_{k-1}$  is the linear map defined on this basis through  $\partial(\Delta) := \Gamma_1 + \Gamma_2 + \cdots + \Gamma_k$ , where the  $\Gamma_i$  are the  $(k-1)$ -element subsets of  $\Delta$ . Thus, we obtain a chain

$$0 \leftarrow M_0 \leftarrow M_1 \leftarrow \cdots \leftarrow M_{k-1} \leftarrow M_k \leftarrow M_{k+1} \leftarrow \cdots \leftarrow M_n \leftarrow 0$$

of inclusion maps. In non-zero characteristic such chains have interesting homological properties which have been examined in earlier papers (Mnukhin and Siemons, 1996). The purpose of this note is to study generators for the homology modules when  $R$  is a field of characteristic  $p \geq n$ .

---

## 1. Inclusion maps

Let  $\Omega$  be a set of finite size  $n$  and  $R$  a field. For  $k \leq n$  consider the  $R$ -vector space  $M_k$  which has  $k$ -element subsets of  $\Omega$  as basis. So  $M_k$  consists of all formal sums  $f = \sum_{|\Delta|=k} r_\Delta \Delta$  with  $\Delta \subseteq \Omega$  and  $r_\Delta \in R$ . The inclusion map  $\partial: M_k \rightarrow M_{k-1}$  is the linear map defined on this basis through  $\partial(\Delta) := \Gamma_1 + \Gamma_2 + \cdots + \Gamma_k$ , where the  $\Gamma_i$  are the  $(k-1)$ -element subsets of  $\Delta$ . So we have a chain of inclusion maps

$$\mathcal{M}: 0 \leftarrow M_0 \leftarrow M_1 \leftarrow \cdots \leftarrow M_{k-1} \leftarrow M_k \leftarrow M_{k+1} \leftarrow \cdots \leftarrow M_n \leftarrow 0.$$

This paper is a continuation of the work in [9,10] with Mnukhin [8], where we have studied such sequences when  $R$  is a field of non-zero characteristic. The following simple observation is crucial: for any integer  $j \geq 1$  we have  $\partial^j(\Delta) = j! \sum \Gamma$  where the summation runs over all  $\Gamma \subset \Delta$  with  $|\Gamma| + j = |\Delta|$ . So if  $R$  has characteristic  $p > 0$ , then  $\partial^j$  is the zero map if and only if  $j \geq p$ . This means that

$$\mathcal{M}_{k,i}: \cdots \leftarrow M_{k-i-p} \leftarrow M_{k-p} \leftarrow M_{k-i} \leftarrow M_k \leftarrow M_{k-i+p} \leftarrow M_{k+p} \leftarrow \cdots$$

---

\* Tel.: +44-1603-592578; fax: +44-1603-259515; e-mail: j.siemons@uea.ac.uk.

is a homological sequence for any  $k$  and any  $1 \leq i < p$ . (Here each arrow is the corresponding power of  $\partial$  and it is convenient to put  $M_j = 0$  for  $j < 0$  and  $j > n$ .) In [10] we have shown that  $\mathcal{M}_{k,i}$  is even exact, except possibly at a single term in the ‘middle’, the precise statement is Proposition 2.2 in the next section.

For such middle terms there will in general be non-trivial homology modules and the purpose of this note is to construct generating sets for these modules when  $R$  has characteristic  $p \geq n$ . Here  $\mathcal{M}_{k,i}$  simply becomes  $0 = M_{k-p} \leftarrow M_{k-i} \leftarrow M_k \leftarrow M_{k-i+p} = 0$  and so the task is to investigate the kernel of the map  $\partial^i: M_k \rightarrow M_{k-i}$ . Throughout this subspace will be denoted by  $K_{k,i}$ . To state our result we need some additional notation. First we require certain subsets of  $M_k$ . The precise meaning of the following expressions is explained in Section 2:

$$C_{k,j} := \{(\alpha_1 - \beta_1) \cup \cdots \cup (\alpha_j - \beta_j) \cup \Gamma : \Gamma \subseteq \Omega, |\Gamma| = k - j, \\ \alpha_s, \beta_t \in \Omega \setminus \Gamma \text{ pairwise distinct}\},$$

and

$$C_{k,j}^* := \{(\alpha_1 - \beta_1) \cup \cdots \cup (\alpha_{j-1} - \beta_{j-1}) \cup (\Gamma - \Gamma^*) : \Gamma, \Gamma^* \subseteq \Omega, \\ |\Gamma^*| = |\Gamma| = k - j + 1, \alpha_s, \beta_t \in \Omega \setminus (\Gamma \cup \Gamma^*) \text{ pairwise distinct}\}.$$

Further, if  $f = \sum r_\Delta \Delta$  then the *weight* of  $f$  is  $w(f) := |\{\Delta: r_\Delta \neq 0\}|$  and the *support* of  $f$  is  $\text{supp}(f) := \bigcup_{r_\Delta \neq 0} \Delta$ . The *minimum weight*  $w_{k,i} := \min\{w(f): 0 \neq f \in K_{k,i}\}$  and the *minimum support size*  $s_{k,i} := \min\{|\text{supp}(f)|: 0 \neq f \in K_{k,i}\}$  then are invariants of  $K_{k,i}$ .

**Theorem.** *Let  $\Omega$  be a set of size  $n$  and  $R$  a field of characteristic  $p \geq n$ . Let  $1 \leq i \leq k$  and  $i < p$  be given. Then  $K_{k,i} \neq 0$  iff  $2k - i + 1 \leq n$ . For  $2k - i + 1 \leq n$  we have  $\dim K_{k,i} = \binom{n}{k} - \binom{n}{k-i}$  and the following hold:*

- (i)  $s_{k,i} = 2k - i + 1$ ,
- (ii)  $K_{k,i}$  is generated by  $C_{k,k-i+1}$ ,
- (iii)  $w_{k,i} = 2^{k-i+1}$  and  $w(x) = 2^{k-i+1}$  for  $x \in K_{k,i}$  iff  $x$  is a scalar multiple of some element in  $C_{k,k-i+1}$  or in  $C_{k,k-i+1}^*$ , and
- (iv) If  $2k \leq n$  and  $n < p$  then  $M_k = K_{k,k+1} = A_0 + A_1 + \cdots + A_k$  with irreducible  $\text{Sym}(\Omega)$ -modules  $A_i$  and the sum can be arranged so that if  $0 \leq i \leq k$  then  $M_{k-i}$  is isomorphic to  $A_0 + A_1 + \cdots + A_i$  and  $K_{k,i}$  is isomorphic to  $A_{i+1} + \cdots + A_k$ .

We remark that all statements in this theorem remain true identically in fields of characteristic 0. Part (ii) then is a theorem of Graver and Jurkat [5]; see also Graham et al. [4] and (iii) is a result of Frankl and Pach [3] which states that  $w_{k,i} = 2^{k-i+1}$  in characteristic 0. Our proof for characteristic  $p \geq n$  applies to characteristic 0 too which gives a new proof and an improvement on the Frankl and Pach theorem. Finally, part (iv) for characteristic 0 is a well-known fact from the representation theory of symmetric groups acting on subsets.

Coming back to the question of homologies in  $\mathcal{M}_{k,i}$ , it is important to realise that for  $p \geq n$  the homology modules are just the  $K_{k,i}$ . While their generators have the same form as in characteristic zero there the interpretation as homologies does not make any sense. In a forthcoming paper [2] we have determined, among many other things, the homology modules for primes  $2 < p < n$ . There the situation is different in many respects, but just the same expressions appear again as generators for the homologies. This is not entirely surprising as these modules are closely related to the polytabloids and Specht modules arising in the representation theory of the symmetric groups.

Apart from representation theory there are other application. One such is the construction of designs, as follows: A  $t - (n, k, \lambda)$  design on  $\Omega$  can be represented by  $f = \sum r_A \Delta \in M_k$ , where  $r_A$  is 1 if  $\Delta$  is a block and 0 otherwise. Being a design means that  $\partial^{k-t}(f) = \lambda(k-t)! \sum_{|F|=t} \Gamma$  and so if  $f, f^*$  are two  $t - (v, k, \lambda)$  designs then  $f - f^*$  belongs to  $K_{k,k-t}$ . Therefore elements of  $K_{k,i}$  are often called null-designs. Lefmann [6] has extended the notion of null-design to other classes of ranked partially ordered sets. In particular, the weight bound (iii) of the theorem has been generalised to projective and affine spaces and to partition lattices.

An important connection exists also to the reconstruction theory of graphs and other combinatorial structures. Müller's condition [11], for instance, a powerful criterion on the edge reconstructibility of graphs with sufficiently many edges, is a direct consequence of the weight bound for the  $K_{k,i}$ . The extensive survey paper [8] by Mnukhin explores this connection and is an excellent reference to this research area. About reconstruction problems see the paper of Alon et al. [1].

## 2. The set calculus

We are going to introduce some kind of calculus which will allow us to deal with collections of subsets in an efficient way. So let  $R$  be some field of arbitrary characteristic and  $\Omega$  a finite set. Then  $2^\Omega$  is the collection of subsets of  $\Omega$  and  $R2^\Omega$  denotes the vector space with  $2^\Omega$  as basis. The operation of set union can be extended to  $R2^\Omega$ : If  $f = \sum f_A \Delta$  and  $g = \sum g_\Gamma \Gamma$ , put  $f \cup g := \sum_{\Delta, \Gamma} f_A g_\Gamma (\Delta \cup \Gamma)$ . It is easy to see that  $R2^\Omega$  equipped with the  $\cup$ -product is an associative algebra with the empty set as 1.

The fundamental relation between the inclusion map and the  $\cup$ -product is the *product rule*: If  $f$  and  $g$  are disjoint elements — by this we mean that  $\text{supp}(f)$  and  $\text{supp}(g)$  are disjoint sets — then

$$\partial(f \cup g) = (\partial f) \cup g + f \cup (\partial g).$$

Very useful and similarly evident is *division with remainder*: If  $f \in M_k$  and  $\alpha \in \text{supp}(f)$ , then there are unique elements  $a \in M_{k-1}$  and  $b \in M_k$  such that  $f = \alpha \cup a + b$  and  $\alpha$  does not belong to  $\text{supp}(b)$ . For the remainder we will use these basic facts without further explanation.

For  $1 \leq i \leq k$  let  $K_{k,i}$  denote the kernel of  $\partial^i: M_k \rightarrow M_{k-i}$ . To exhibit certain important standard elements in  $K_{k,i}$  let  $j \leq k$  and consider the set

$$C_{k,j} := \{(\alpha_1 - \beta_1) \cup \cdots \cup (\alpha_j - \beta_j) \cup \{\gamma_{j+1}, \dots, \gamma_k\} : \\ \alpha_s, \beta_t, \gamma_u \text{ pairwise distinct}\}.$$

mentioned before. Its elements have support size  $k + j$  and weight  $2^j$ . From the product rule it follows immediately that  $C_{k,j} \subseteq K_{k,i}$  whenever  $k - i < j$  and as  $(\alpha_1 - \beta_1) \cup \cdots \cup (\alpha_j - \beta_j) \cup \{\gamma_{j+1}, \gamma_{j+2}, \dots, \gamma_k\} - (\alpha_1 - \beta_1) \cup \cdots \cup (\alpha_j - \beta_j) \cup \{\gamma_{j+1}^*, \gamma_{j+2}, \dots, \gamma_k\} = (\alpha_1 - \beta_1) \cup \cdots \cup (\alpha_j - \beta_j) \cup (\gamma_{j+1} - \gamma_{j+1}^*) \cup \{\gamma_{j+2}, \dots, \gamma_k\}$  we see that  $\langle C_{k,k} \rangle \subseteq \langle C_{k,k-1} \rangle \subseteq \cdots \subseteq \langle C_{k,0} \rangle = M_k$ .

The elements of  $C_{k,k}$  have a particularly nice geometric interpretation. When  $k = 3$ , for instance, then  $(\alpha_1 - \beta_1) \cup (\alpha_2 - \beta_2) \cup (\alpha_3 - \beta_3)$  represents the alternately signed faces of an octahedron which one can view as the dual of a three-dimensional cube. By analogy,  $(\alpha_1 - \beta_1) \cup \cdots \cup (\alpha_k - \beta_k)$  are the alternating faces of the dual of the  $k$ -dimensional cube. Equivalently, one can view these expressions as the polytabloids featuring in the representation theory of symmetric groups.

**Proposition 2.1** (Mnukhin and Siemons [10, Theorem 2.2]). *If  $R$  is an arbitrary ring then  $K_{k,i}$  is generated by elements of the form  $h \cup \Delta$  where  $h$  belongs to  $K_{k-i+1,1}$  and where  $\Delta$  is an  $(i-1)$ -element set disjoint from  $h$ . Furthermore,  $K_{k,i}$  is generated by elements of support size at most  $2k - i + 1$ .*

If  $R$  is a field of characteristic  $p \neq 0$  and  $|\Omega| = n$  let us consider the sequence

$$\mathcal{M}_{k,i} : \cdots \leftarrow M_{k-i-p} \leftarrow M_{k-p} \leftarrow M_{k-i} \leftarrow M_k \leftarrow M_{k-i+p} \leftarrow M_{k+p} \leftarrow \cdots$$

in which each arrow is the corresponding power of  $\partial$  and where we put  $M_k = 0$  for  $k < 0$  or  $k > n$ . As mentioned before,  $\partial^j(\Delta) = j! \sum \Gamma$  where the sum is over all  $\Gamma \subset \Delta$  with  $|\Gamma| + j = |\Delta|$  and we see that  $\partial^j$  is the zero map if and only if  $j \geq p$ .

In other words,  $\mathcal{M}_{k,i}$  is always homological. The next results are fundamental for this paper. Binomial coefficients  $\binom{n}{s}$  are zero for  $s < 0$  and for  $s > n$ .

**Proposition 2.2** (Mnukhin and Siemons [10, Theorem 5.3]). *Let  $1 \leq i < p$  and  $i < k$ . If  $p = 2$ , then  $\mathcal{M}_{k,i}$  is exact. If  $p \geq 3$ , then  $\mathcal{M}_{k,i}$  is exact everywhere except possibly at  $M_{t-p} \leftarrow M_s \leftarrow M_t$  when  $n < s + t < n + p$ . Let  $K$  be the kernel of  $M_{t-p} \leftarrow M_s$  and  $I \subseteq M_s$  the image of  $M_s \leftarrow M_t$ . Then  $\dim K/I = \sum_{j \in \mathbb{Z}} \binom{n}{s+jp} - \binom{n}{t+jp} = |\sum_{j \in \mathbb{Z}} \binom{n}{k+jp} - \binom{n}{k-i+jp}|$ .*

Accordingly, for  $p \geq 3$  we call a pair  $(k, i)$  a *lower term* if  $k + k - i + p \leq n$ , a *middle term* if  $n < k + k - i + p < n + p$ , and an *upper term* if  $n + p \leq k + k - i + p$ . For this paper a useful corollary is

**Proposition 2.3.** *Let  $1 \leq i < p$  and  $i < k$ . Then  $K_{k,i} = \partial^{p-i}(M_{k-i+p})$  unless  $p \geq 3$  and  $(k, i)$  is a middle term. In particular,  $K_{k,i} \neq 0$  if  $k - i + p \leq n$ .*

### 3. Fields of characteristic at least $n$

The theorem will be proved in a sequence of lemmas. So let  $\Omega$  have size  $n$  and suppose that  $R$  is a field of characteristic  $p \geq n$ . Let  $1 \leq i \leq k$  be given integers. For  $i = k$  the situation is quite clear so we will assume  $i < k$ . The sequence  $\mathcal{M}_{k,i}$  now becomes  $0 = M_{k-p} \leftarrow M_{k-i} \leftarrow M_k \leftarrow M_{k-i+p} = 0$  and  $(k, i)$  is a middle term if and only if  $k + k - i < n$ . By Propositions 2.2 and 2.3 we have  $K_{k,i} = 0$  if  $2k - i \geq n$  while  $\dim K_{k,i} = \binom{n}{k} - \binom{n}{k-i}$  if  $2k - i < n$ . In particular, the minimum support size in  $K_{k,i}$  is  $2k - i + 1$ . Hence,

**Lemma 3.1.** *Let  $R$  be a field of characteristic  $p \geq n$  and let  $1 \leq i < k$  be given. Then  $K_{k,i} \neq 0$  iff  $2k - i + 1 \leq n$ . If  $2k - i + 1 \leq n$ , then  $\dim K_{k,i} = \binom{n}{k} - \binom{n}{k-i}$  and the minimum support size in  $K_{k,i}$  is  $2k - i + 1$ .*

Next we are going to show that the sets  $C_{k,j}$  defined in Section 2 generate the kernels. In view of Proposition 2.1 it is sufficient to consider  $K_{k,1}$ . The argument we present is the one of Graham et al. [4] and applies also when  $R$  has characteristic zero.

We claim that  $C_{k,k}$  generates  $K_{k,1}$ . To show this proceed by induction on  $k$ , and for fixed  $k$  on the support size. So suppose the claim is true for all values  $< k$  and support sizes  $< m$ . Let  $0 \neq x \in K_{k,1}$  have  $|\text{supp}(x)| =: m$  where  $2k \leq m \leq n$  by Lemma 3.1. For  $\alpha \in \text{supp}(x)$  we write  $x = \alpha \cup a + b$  where  $0 \neq a \in M_{k-1}$  so that  $0 = \partial(x) = \alpha \cup \partial(a) + (a + \partial(b))$ . Hence  $\partial(a) = 0 = a + \partial(b)$  and as  $a \in K_{k-1,1}$  induction applies. So we can write  $a = \sum_{\lambda} r_{\lambda} c_{\lambda}$  with  $r_{\lambda} \in R$ ,  $c_{\lambda} \in C_{k-1,k-1}$  and  $\text{supp}(c_{\lambda}) \subset \text{supp}(x)$ .

As  $\text{supp}(c_{\lambda})$  has size  $2(k-1)$  we let  $\alpha_{\lambda} \neq \alpha$  be a point in  $\text{supp}(x) \setminus \text{supp}(c_{\lambda})$ . Consider  $y = x - \sum_{\lambda} (\alpha - \alpha_{\lambda}) \cup r_{\lambda} c_{\lambda} = \alpha \cup a + b - \sum_{\lambda} (\alpha - \alpha_{\lambda}) \cup r_{\lambda} c_{\lambda} = b - \sum_{\lambda} \alpha_{\lambda} \cup r_{\lambda} c_{\lambda}$ . Then firstly  $\text{supp}(y) \subseteq \text{supp}(x) \setminus \{\alpha\}$  and secondly  $\partial(y) = 0$  as  $0 = a + \partial(b)$ . So, by induction,  $x$  can be expressed in the desired form and by Proposition 2.1 we have

**Lemma 3.2.** *If  $R$  has characteristic  $p \geq n$  let  $1 \leq i < k$ ,  $i < p$  be given and suppose that  $2k - i + 1 \leq n$ . Then  $K_{k,i}$  is generated by  $C_{k,k-i+1}$ .*

It is worth pointing out that the proof of this lemma is characteristic free and depends only on the knowledge of the minimal support sizes.

**Lemma 3.3.** *Let  $R$  be a field of characteristic  $p$  and suppose that  $1 \leq i \leq k < p$  are given. If  $0 \neq x \in K_{k,i}$  then  $w(x) \geq 2^{k-i+1}$  with equality if and only if there is some  $0 \neq c \in R$  with either*

- (i)  $x = c(\alpha_1 - \beta_1) \cup \dots \cup (\alpha_r - \beta_r) \cup \Gamma$  with  $\alpha_s, \beta_t \notin \Gamma$  pairwise disjoint for  $1 \leq s, t \leq r$  and  $r = k - i + 1$ ,  $|\Gamma| = i - 1$ , or
- (ii)  $x = c(\alpha_1 - \beta_1) \cup \dots \cup (\alpha_r - \beta_r) \cup (\Gamma - \Gamma^*)$  with  $\alpha_s, \beta_t \notin \Gamma \cup \Gamma^*$  pairwise disjoint for  $1 \leq s, t \leq r$  and  $r = k - i$ ,  $|\Gamma| = |\Gamma^*| = i$ .

In other words, up to scalars the minimum weight vectors of  $K_{k,i}$  are precisely the elements of  $C_{k,k-i+1}$  and  $C_{k,k-i+1}^*$ . The special case  $i = 1$ , in a different context, has been considered in [12, Proposition 2].

**Proof.** We apply induction on  $k$  and for fixed  $k$  on  $k - i$ , the result being obvious when  $k = 1$  and  $k = i$ . So suppose that the lemma is true for all values  $< k$  and  $< k - i$ . Let  $0 \neq x \in K_{k,i}$  with  $w(x) \leq 2^{k-i+1}$ . It suffices to show that  $w(x) = 2^{k-i+1}$  and that  $x$  has the stated form.

Let  $\alpha \in \text{supp}(x)$  and write  $x = \alpha \cup a + b$ , where  $0 \neq a \in M_{k-1}$  and  $b \in M_k$ . Then  $\partial^i(x) = \alpha \cup \partial^i(a) + i\partial^{i-1}(a) + \partial^i(b)$ . If  $b = 0$ , then  $w(x) = w(a)$  and  $\partial^{i-1}(a) = 0$  as  $i < p$ . Thus  $a \in K_{k-1,i-1}$ . By induction  $w(a) \geq 2^{(k-1)-(i-1)+1} \geq w(x)$  so that  $w(a) = 2^{(k-1)-(i-1)+1}$  and  $a$  satisfies the conclusion of the lemma. But then the same is true for  $x$ .

Now assume that  $b \neq 0$ . From  $0 = \partial^i(x)$  it follows that  $0 = \partial^i(a)$ ,  $-i\partial^{i-1}(a) = \partial^i(b)$  and hence  $\partial^{i+1}(b) = 0$ . Therefore  $a \in K_{k-1,i}$ ,  $b \in K_{k,i+1}$  and by induction  $w(a) \geq 2^{(k-1)-i+1}$  and  $w(b) \geq 2^{k-(i+1)+1}$ . However,  $2^{k-i+1} \geq w(x) = w(a) + w(b) \geq 2^{k-i+1}$  shows that  $w(a) = w(b) = 2^{k-(i+1)+1}$  and  $w(x) = 2^{k-i+1}$ .

Furthermore,  $a$  and  $b$  satisfy the conclusion of the lemma. Therefore also  $a^* := \alpha \cup a$  is either of type (i),  $a^* = c_1(\alpha_1 - \beta_1) \cup \dots \cup (\alpha_s - \beta_s) \cup \Gamma$  with  $s = k - i$ ,  $|\Gamma| = i$ , or of type (ii),  $a^* = c_1(\alpha_1 - \beta_1) \cup \dots \cup (\alpha_s - \beta_s) \cup (\Gamma - \Gamma^*)$  with  $s = k - i - 1$ ,  $|\Gamma| = |\Gamma^*| = i + 1$ . The same applies to  $b$  so that either (i)  $b = c_2(\gamma_1 - \delta_1) \cup \dots \cup (\gamma_t - \delta_t) \cup \Delta$  with  $t = k - i$ ,  $|\Delta| = i$ , or (ii)  $b = c_2(\gamma_1 - \delta_1) \cup \dots \cup (\gamma_t - \delta_t) \cup (\Delta - \Delta^*)$  with  $t = k - i - 1$ ,  $|\Delta| = |\Delta^*| = i + 1$ .

Now as  $\partial^i(x) = 0$  we have  $-\partial^i(a^*) = \partial^i(b)$ . Computing these terms, we find that  $\partial^i(a^*)$  is either  $i!c_1(\alpha_1 - \beta_1) \cup \dots \cup (\alpha_s - \beta_s)$  or  $i!c_2(\alpha_1 - \beta_1) \cup \dots \cup (\alpha_s - \beta_s) \cup (\bar{\Gamma} - \bar{\Gamma}^*)$  where  $\bar{\Gamma} = (i!)^{-1}\partial^i(\Gamma)$  denotes the sum of all points in  $\Gamma$ , etc. Similarly,  $\partial^i(b)$  is either  $i!c_2(\gamma_1 - \delta_1) \cup \dots \cup (\gamma_t - \delta_t)$  or  $i!c_2(\gamma_1 - \delta_1) \cup \dots \cup (\gamma_t - \delta_t) \cup (\bar{\Delta} - \bar{\Delta}^*)$ . Factorisation into disjoint terms is unique, as for polynomials in several variables. From  $-\partial^i(a^*) = \partial^i(b)$  it follows immediately that  $a^*$  and  $b$  are of the same type and in both cases that  $s = t$ ,  $c_1 = c_2$  and  $(\alpha_j - \beta_j) = (\gamma_j - \delta_j)$  after a suitable rearrangement. Further,  $a^*$  and  $b$  cannot be of type (ii), for  $(\bar{\Gamma} - \bar{\Gamma}^*) = (\bar{\Delta} - \bar{\Delta}^*)$  implies  $\Gamma = \Delta$  and  $\Gamma^* = \Delta^*$  so that  $a^* = -b$  and  $x = 0$ .

So we have  $a^* = c_1(\alpha_1 - \beta_1) \cup \dots \cup (\alpha_s - \beta_s) \cup \Gamma$  and  $b = -c_1(\alpha_1 - \beta_1) \cup \dots \cup (\alpha_s - \beta_s) \cup \Delta$  which gives  $x = c_1(\alpha_1 - \beta_1) \cup \dots \cup (\alpha_s - \beta_s) \cup (\Gamma - \Delta)$  and the lemma is proved.  $\square$

To complete the proof of the theorem, consider  $R2^\Omega$  and  $K_{k,j}$  as  $RSym(\Omega)$ -modules. As  $p$  does not divide  $|\text{Sym}(\Omega)|$  all modules are completely reducible by Maschke's theorem and so the elementary theory of permutation modules is just as in the characteristic 0 case. Hence, if  $\pi = \sum n_i \chi_i$  is the decomposition of a permutation character into irreducible characters  $\chi_i$ , where  $\chi_1$  is the identity character, then  $n_1$  is the number of orbits and  $\sum n_i^2$  is the permutation rank of the group.

Considering  $\text{Sym}(\Omega)$  as a permutation group on the  $k$ -element subsets of  $\Omega$ , it is clear that this action has rank  $k + 1$ . Therefore  $M_k$  decomposes into at most  $k + 1$  irreducible

constituents. On the other hand, the sequence  $0 \subset K_{k,1} \subset K_{k,2} \subset \cdots \subset K_{k,k} \subset K_{k,k+1} = M_k$  has  $k+1$  distinct non-zero terms as by Lemma 3.1  $\dim K_{k,j} \neq \dim K_{k,j+1}$ . Hence  $M_k = A_0 + A_1 + \cdots + A_k$  decomposes into precisely  $k+1$  non-isomorphic irreducible  $\text{Sym}(\Omega)$ -modules. For the remainder observe that  $\partial^i$  maps  $0 \subset K_{k,1} \subset K_{k,2} \subset \cdots \subset K_{k,i} \subset K_{k,i+1} \subset \cdots \subset K_{k,k} \subset K_{k,k+1} = M_k$  to  $0 \subset K_{k-i,1} \subset \cdots \subset K_{k-i,k-i} \subset K_{k-i,k-i+1} = M_{k-i}$  with kernel  $K_{k,i}$  and by Lemma 3.1 this map is surjective.  $\square$

## References

- [1] N. Alon, Y. Caro, I. Krasikov and Y. Roditty, Combinatorial reconstruction problems, *J. Combin. Theory B* 47 (1989) 153–161.
- [2] S. Bell, P. Jones and I.J. Siemons, On modular homology in the Boolean algebra II, to appear.
- [3] P. Frankl and J. Pach, On the number of sets in a null-design, *European J. Combin.* 4 (1983) 21–23.
- [4] R.L. Graham, S.Y.R. Li and W.C. Li, On the structure of  $t$ -designs, *SIAM J. Algebraic Discrete Methods* 1 (1980) 8–14.
- [5] J.E. Graver and W.B. Jurkat, The module structure of integral designs, *J. Combin. Theory A* 15 (1973) 75–90.
- [6] H. Lefmann, An extremal problem for Graham–Rothschild parameter words, *Combinatorica* 9 (2) (1989) 153–160.
- [7] N. Linial and B.L. Rothschild, Incidence matrices of subsets — a rank formula, *SIAM J. Algebraic Discrete Methods* 2 (1981) 330–340.
- [8] V.B. Mnukhin, The  $k$ -orbit reconstruction and the orbit algebra, *Acta Appl. Math.* 29 (1992) 83–117.
- [9] V.B. Mnukhin and I.J. Siemons, On modular homology in the Boolean algebra, *J. Algebra* 179 (1996) 191–199.
- [10] V.B. Mnukhin and I.J. Siemons, On the modular theory of inclusion maps and group actions, *J. Combin. Theory Ser. A* 74 (1996) 287–300.
- [11] V. Müller, The edge reconstruction hypothesis is true for graphs with more than  $n \log_2 n$  edges, *J. Combin. Theory B* 22 (1977) 281–283.
- [12] I.J. Siemons, Decompositions of modules associated to finite-partially ordered sets, *European J. Combin.* 15 (1994) 53–56.